INFORMATION SYSTEMS AUDIT OF

THE DB2 DATA BASE MANAGEMENT SYSTEM

FEDERAL DEPOSIT INSURANCE CORPORATION

OFFICE OF INSPECTOR GENERAL

April 10, 1996

INFORMATION SYSTEMS AUDIT OF THE DB2 DATA BASE MANAGEMENT SYSTEM

TABLE OF CONTENTS

FDIC
Federal Deposit Insurance Corporation
Washington, D.C. 20429 Office of Inspector General

OFFICIAL AUDIT RELEASE **April 10, 1996**
DETAIL AUDIT REPORT

MEMORANDUM TO: Donald C. Demitros, Director
Division of Information Resources Management

FROM: Richard E. Wingate
Assistant Inspector General

SUBJECT: Information Systems Audit Report on the
DB2 Data Base Management System

As a part of our responsibility for providing independent audits of corporate automated systems for the Board of Directors, we have completed an information systems audit of the DB2 Data Base Management System. The audit was initiated on August 16, 1995, and was performed by the Operational Systems Audit Branch. Audit field work was completed on January 17, 1996. We issued seven Preliminary Statements of Audit Condition and Corrective Action to the Division of Information Resources Management (DIRM) on January 18, 1996 for written responses. Due to the length of DIRM's responses, we have incorporated excerpts from the responses into the details section of the draft report. A draft report was issued to DIRM on March 20, 1996.

The DB2 Data Base Management System is a product of the International Business Machines (IBM) Corporation. Purchased by FDIC in 1991, DB2 provides desirable enhancements over the hierarchical data base system in use. DB2 is a relational data base that stores data in tables accessed by field value only. It provides effective controls over access, concurrency, and the integrity of data. Other benefits of DB2 is the ability to reduce data redundancy, increase data accessability, and enable effective recovery.

The number of new or redesigned application systems using DB2 has increased steadily since its purchase. Mainframe application systems presently supported by DB2 include the Personnel Access Request System (PARS), Payroll/Personnel, Negotiable Collateral System, the National Contractor System, and the Telephone Monitoring and Reporting System. In addition, efforts are underway to upgrade major Corporate systems (general ledger, travel, accounts payable, etc.) purchased from Walker Interactive Products Systems to DB2 managed systems recently developed by Walker.

The popularity of DB2 has also led to the availability of a significant number of software support packages distributed by third party vendors. FDIC has purchased several of these packages to enhance query capabilities, performance monitoring, and maintenance. In addition,

almost every major application programming language used in the market today supports DB2's Structured Query Language.

AUDIT SCOPE AND OBJECTIVES

The audit scope included system software and utilities which directly make-up and support the DB2 System. The audit also included a limited review of application systems running under DB2 in production and development. Future OIG audits will evaluate the application systems running under DB2 in greater depth. The objectives of this audit were to: 1) evaluate the security of the DB2 environment; 2) evaluate the effectiveness of internal access controls over data; and 3) determine the effectiveness of DB2 maintenance.

The audit was performed in accordance with generally accepted auditing standards and the standards for performance audits contained in the U.S. General Accounting Office Government Auditing Standards: 1994 Revision as promulgated by the Comptroller General of the United States.

CONCLUSIONS

A detailed discussion of each condition and recommendation, along with management's response, is presented in the audit report. Items which we consider particularly significant are summarized below under each audit objective.

Security of the DB2 environment

Security of the DB2 environment is adequate. We found that DB2 system libraries and subsystem files are generally protected from inadvertent or malicious access. The primary means of protecting mainframe software systems and data is provided by the Access Control Facility (ACF2). We found a few instances in which ACF2 rule sets needed to be modified to prevent unauthorized access using powerful utilities. These utilities have the capability of directly accessing DB2 files without regard for DB2's security or operational status. The utilities could be used to browse and modify production data bases and could potentially disrupt operations of the DB2 system.

Effectiveness of internal access controls over data

Internal access controls are fair. Privileges granted to DB2 users were not sufficiently limited to provide proper separation of duties and to prevent browsing of sensitive data. The related audit conditions are summarized below:

- **Data Base Administrator Privileges Should Be Judiciously Controlled (Condition 3)**

  Data base administrator privileges have been granted to Data

Base Unit (DBU) personnel although such access is not needed on a daily basis.

The assignment of data base administrator privileges to a group ID provides users within the group, unrestricted access to all resources associated with the specific data base. Users assigned as systems administrators have unrestricted access to all systems and all data base resources. We found that the group IDs for the data base administrators of each data base generally contained from 9 to 12 DBU employees. Therefore, these employees can access all data bases using powerful administrator privileges. In addition, two systems install administrators and five system administrators also have data base administrator privileges. Documentation showing the assignments of DBU personnel generally limited administrative controls of each data base to only one administrator and two backups. Additionally, we determined: (1) two DBU employees had DB2 administrators privileges but were not assigned DB2 responsibilities; (2) one DB2 administrator possessed the powerful system administrator privileges without the equivalent responsibilities; (3) the LAMIS System's two DB2 data bases that are managed by the System Support Group were assigned 6 data base administrators even though the required support work was minimal; and (4) the National Finance Center (NFC) support data bases included an ID for a data base administrator who no longer works for FDIC.

* * * Auditee Response * * *

DIRM concurs with the philosophy of the recommendation; However, current operational policy precludes immediate implementation of the recommendation.

The two employees of DBU who had data base administration privileges but were not assigned to specific administration tasks have been provided lesser access privileges. The DB2 administrator with SYSADM privileges, who does not perform this function, has had the authorization removed. The system administrator who no longer works for the FDIC has had the authorization removed.

The Data Base Unit (DBU) and Security Administration Section (SAS) will conduct a feasibility study to determine if the "fire call" procedures previously used by the RTC are transferrable to the FDIC, in terms of issuing emergency authorizations in a very short timeframe, and if these procedures will meet the operational needs of the DBU. If feasible, DBU and SAS will work together to implement the procedures, change the current policy, and comply with the recommendation. The target completion date for this feasibility study is 5/31/96.

- **Data Changes By DB2 Administrators (Condition 4)**

  DB2 administrators have the authorization to insert, delete and update nearly any production data base using DB2 utilities and third party vendor software packages. In emergency situations, this level of access may be required for instance, to repair or correct data outside of the application environment. However, we noted instances in which routine changes were carried out by the administrator that should have been made through the respective application resource.

  * * * Auditee Response * * *

  DIRM concurs with this finding/recommendation and notes the following:

  - The data changes made by DBU to the application cited in this finding, PARS, were emergency in nature. PARS is a critical personnel application which processes personnel changes being sent to the National Finance Center (NFC). Because of the disruption to employees if PARS processing were interrupted, the DBU has made corrections to corrupted PARS data upon written request of the data steward for PARS. All changes are logged to the DB2 active log and documented with the written change control document from the data steward.

  DBU issued a memo to all DBU DBAs dated 2/6/96 that addressed the new procedures all DBAs should follow to ensure that only emergency data changes are made by DBU staff. DBU will issue a memorandum to application units by 4/15/96 stating that, except in emergencies certified by the data steward, no data changes will be made by DBU staff.

- **Browsing of Data Needs Tighter Restrictions (Condition 5)**

  Access authorizations granted to users through DB2's system security catalogues allowed viewing of sensitive data. Nine views to one data base included in our review contained sensitive bank information which were granted “PUBLIC” access.

  * * * Auditee Response * * *

  DIRM concurs with this recommendation. The nine views cited were dropped on 1/26/96. This “sensitive bank information” was a test migration between DATACOM and DB2, and was approved by the data steward.

  Currently DBU internally reviews PUBLIC access on a monthly basis, to ensure that any data declared by the data steward to be sensitive is <u>not</u> granted PUBLIC access. As a part of the

project development, DB2 DBAs will continue to coordinate with the project managers to implement the appropriate accesses, PUBLIC or otherwise.

Overall effectiveness of DB2 maintenance

Maintenance of the DB2 system is adequate, but as more application data bases are added and as they grow in size, performance could suffer unless improvements are made. Our technical analysis of installation parameters, system authorization catalogues, and the ACF2 group ID file, resulted in recommendations for future improvements in maintenance that should be made prior to committing to other, more expensive, alternatives. In addition, we found that some data bases were not under the auspices of DBU. Our review disclosed that the quality of maintenance provided these data bases was not sufficient to ensure adequate reliability and recovery. To ensure a high quality of maintenance, we believe that the administration of DB2 production data bases should be centralized in DBU. We also recommended that maintenance procedures be sufficiently documented in light of potential staff changes that could occur as a result of reorganization or downsizing.

AUDIT PROCEDURES

The audit procedures and techniques used to achieve the audit objectives included the following: (1) review of the system parameters used to install DB2 in the five subsystems currently used by FDIC; (2) review of ACF2 rule sets and resource sets that are applicable to DB2 operational security; (3) analyzed the capabilities of DB2 supplied utilities as well as third party utility packages capable of accessing DB2 system catalogs and application data bases; (4) developed Query Management Facility (QMF) code to select, test, and evaluate system catalogues and data base tables; and (5) interviewed systems and data base administrators.

AUDIT CONDITIONS, RECOMMENDATIONS, AND AUDITEE RESPONSES

1. Data Base Management is Not Consolidated Within the Data Base Unit

The management of DB2 production data bases residing on the FDIC mainframe computer system is not fully consolidated within the DBU. As a result, data bases under the management of other units are not being afforded the quality of the automated maintenance and performance routines developed and utilized by DBU to ensure effective operations and recovery.

Our review of two LAMIS databases managed by the System Support Unit found that the back-up procedures were not automated and hence, inconsistently performed. One data base was backed-up less than half the prescribed time. The other was backed-up only two months during

1995, even though the administrator stated standards require full backup every two weeks.

In contrast, DBU uses automated tools that ensure that data bases and other DB2 resources are backed-up every two weeks. DBU provides additional resources not possessed by other units that could more effectively manage the sensitive data bases including:

- DBU uses automated maintenance tools that quickly detect performance problems and inform system administrators of the most effective corrective strategies;

- DBU administrators have the technical expertise to quickly correct DB2 related problems. DBU system and data base administrators are continually trained in techniques to enhance performance and efficiently resolve data base problems. The Systems Support Unit administrator stated data base management was not his highest priority and many times had to relearn even the more basic data base support procedures;

- DBU is supported by automated change control procedures thereby reducing risk of unauthorized program changes;

- DBU procedures granting access to DB2 data are standardized and are managed by separation of duty controls;

- Recovery procedures have been tested for all data bases managed by DBU.

Given the significant growth of DB2 data bases over the next few years including the potential transfer of Resolution Trust Corporation (RTC) data bases, the importance of centralized maintenance and performance tuning is essential to ensuring an adequate response time, consistency in security methodologies, and the ability to timely and fully recover critical systems and data.

Recommendation:

DIRM should develop policy that centralizes DB2 performance and maintenance responsibilities in DBU. DBU should discuss with the various units currently managing production DB2 data bases the logistics for transferring maintenance responsibilities for the data bases to DBU.

Auditee Response:

The DB2 DBA access for the LAMIS Support Unit was removed on 3/15/96. This action placed all of the DB2 DBA functions within DBU. The recent DIRM reorganization addresses the centralization of DB2 DBA functions by placing the functions in a single unit.

2. Off-line Utilities Bypass DB2 Security

ACF2 rules sets governing access to DB2 subsystem objects (system catalogues, data bases and their tables, plans, etc.) are not sufficient to limit access using powerful off-line utilities. These utilities can access DB2 resources outside the control of the DB2 management system, regardless of the operational status of the DB2 systems. As a result, restrictions placed on access to objects by the system and data base administrators using DB2 can be bypassed.

Mainframe system libraries contain a number of powerful utilities capable of accessing DB2 objects. Example of these utilities include DSN1COPY, DSN1PRNT, and IDCAMS. These utilities can be invoked at any time, even if the DB2 system is disabled. The utilities enable users to browse, copy, and write to DB2 objects without being subjected to DB2 restrictions. Modifications could be attempted using these utilities to modify DB2 system catalogues and thereby inappropriately grant access to DB2 objects. In addition, users of these utilities could intentionally or unintentionally disable DB2 operations. Instructions for using these utilities are available to all on-line TSO users.

We reviewed the ACF2 rule sets for system libraries and for the DB2 libraries. The system libraries containing the utilities are open to all users. The DB2 production and development libraries under project code 9102 were open to 89 logon IDs that included a CO-OP student, a unit secretary, and eight test IDs.

Recommendation:

We recommend that DIRM review the ACF2 rule sets for production and development DB2 objects and ensure access to the objects is appropriate and commensurate with authorizations granted by system and data base administrators.

Auditee Response:

The Security Administration Section (SAS) and the Database Unit (DBU) worked together and limited access though the use of ACF2 rule sets to production and development DB2 objects. They also reviewed and limited access to DB2 off-line utilities and other packages capable of disseminating DB2 data base files. SAS and DBU completed these tasks on 3/15/96.

3. Data Base Administrator Privileges Should Be Judiciously Controlled

Data base administrator privileges have been granted to DBU personnel although such access is not needed on a daily basis.

The assignment of data base administrator privileges to a group ID provides users within the group, unrestricted access to all resources

associated with the specific data base. Users assigned as system administrators have unrestricted access to all systems and all data base resources. We found that the group IDs for the data base administrators of each data base generally contained from 9 to 12 DBU employees. Therefore, these employees can access all data bases using powerful administrator privileges. In addition, two systems installation administrators and five system administrators also have data base administrator privileges. Documentation showing the assignments of DBU personnel generally limited administrative controls of each data base to only one administrator and two backups. Additionally, we determined: (1) two DBU employees had DB2 administrators privileges but were not assigned DB2 responsibilities; (2) one DB2 administrator possessed the powerful system administrator privileges without the equivalent responsibilities; (3) the LAMIS System's two DB2 data bases that are managed by the System Support Group were assigned 6 data base administrators even though the required support work was minimal; and (4) the National Finance Center (NFC) support data bases included an ID for a data base administrator who no longer works for FDIC.

Administrator access to production data bases should be limited to only those responsible for their day-to-day maintenance. OIG does recognize exceptions to this separation of duties convention, such as holidays, off-site training, or other events that may limit the number of administrators on call.

Recommendation:

We recommend that DBU limit personnel assigned to group IDs as data base administrators except under unique circumstances such as holidays. Exceptions should be limited to the time period surrounding the circumstances.

Auditee Response:

DIRM concurs with the philosophy of the recommendation; However, current operational policy precludes immediate implementation of the recommendation.

The two employees of DBU who had data base administration privileges but were not assigned to specific administration tasks have been provided lesser access privileges. The DB2 administrator with SYSADM privileges, who does not perform this function, has had the authorization removed. The system administrator who no longer works for the FDIC has had the authorization removed.

The Data Base Unit (DBU) and Security Administration Section (SAS) will conduct a feasibility study to determine if the "fire call" procedures previously used by the RTC are transferrable to the FDIC, in terms of issuing emergency authorizations in a very short timeframe, and if these procedures will meet the operational needs of the DBU. If feasible, DBU

and SAS will work together to implement the procedures, change the current policy, and comply with the recommendation. The target completion date for this feasibility study is 5/31/96.

4. Data Changes By DB2 Administrators

DB2 administrators have the authorization to insert, delete and update nearly any production data base using DB2 utilities and third party vendor software packages. In emergency situations, this level of access may be required for instance, to repair or correct data outside of the application environment. However, we noted instances in which routine changes were carried out by the administrator that should have been made through the respective application resource.

Separation of duty principles require data base administrators to modify table and data base attributes but restrict them from making routine modifications to application data. The primary reason is that automated and manual data integrity controls reside within the application environment to protect the integrity of the data from erroneous or unauthorized data modifications. Data base administrators using "backdoor" access to the tables avoid the data integrity controls and thus increase the risk for inaccurate or unauthorized data revision. Additionally, restricting data modifications from DB2 administrators allows accountability to reside with the application users and not DBU.

Our review of change requests documents for the PARS data base indicate data base administrators modified PARS data directly from the DB2 tables. For example, two change control documents indicate the data base administrator added logon ID 'RC1102' to PARS tables so the employee could assume responsibility to review personnel actions. Other change requests indicate data base administrators adding employees to initiate personnel actions or altering social security numbers of PARS users. Considering the high risk nature of such personnel data, these modifications should not be executed outside the application controls designed to support data reliability and integrity. Additionally, considering that all FDIC financial data bases will soon be managed by DB2 administrators, DBU management should require and document standards that will caution DB2 administrators in making routine modifications to DB2 data.

Recommendation:

DBU management should document standards that will caution DB2 administrators from making routine modifications to data using direct access methods such as SPUFI and QMF. Except in emergencies, data changes such as those described above should be processed through the application, thus limiting accountability for data accuracy to the application users.

Auditee Response:

DIRM concurs with this finding/recommendation and notes the following:

- The data changes made by DBU to the application cited in this finding, PARS, were emergency in nature. PARS is a critical personnel application which processes personnel changes being sent to the National Finance Center (NFC). Because of the disruption to employees if PARS processing were interrupted, the DBU has made corrections to corrupted PATS data upon written request of the data steward for PARS. All changes are logged to the DB2 active log and documented with the written change control document from the data steward.

DBU issued a memo to all DBU DBAs dated 2/6/96 that addressed the new procedures all DBAs should follow to ensure that only emergency data changes are made by DBU staff. DBU will issue a memorandum to application units by 4/15/96 stating that, except in emergencies certified by the data steward, no data changes will be made by DBU staff.

5. Browsing of Data Needs Tighter Restrictions

Access authorizations granted to users through DB2's system security catalogues allowed viewing of some sensitive data.

Nine views to one data base included in our review contained sensitive bank information which were granted "PUBLIC" access. Views are DB2 objects that enable authorized users to access information (columns and rows) in data base tables in a matter specified by the creator of the view. When DB2 objects are granted to "PUBLIC", any user could use one of several available vendor packages (e.g. QMF, BMC software products, or SPUFI) to browse or possibly modify the tables.

Recommendation:

We recommend that the System and data base administrators and the data stewards assigned to their respective application data bases should review DB2 objects granted "PUBLIC" access to ensure that sensitive data cannot be compromised.

Auditee Response:

DIRM concurs with this recommendation. The nine views cited were dropped on 1/26/96. This "sensitive bank information" was a test migration between DATACOM and DB2, and was approved by the data steward.

Currently DBU internally reviews PUBLIC access on a monthly basis, to ensure that any data declared by the data steward to be sensitive is <u>not</u> granted PUBLIC access. As a part of the project development, DB2 DBAs will continue to coordinate with the project managers to implement the appropriate accesses, PUBLIC or otherwise.

6. Installation Performance Parameters and Periodic Maintenance Processes Will Need to Be Refined to Meet Future Workload Requirements

As the number of DB2 application systems increase over the short term, installation performance parameters and maintenance processes will need refining in order to maintain the levels of system performance currently enjoyed by DB2 users. These parameters and processes include the restrictions and maintenance of primary (user logon) and group IDs in DB2, periodic clean-up of system catalogues, placement of restrictions on the use of DB2 objects for on-line ad hoc queries, and the existence of non-business data bases in the production subsystem.

Usage of the DB2 Data Base Management System for production applications is steadily increasing. As familiarity of DB2 increases, more applications will most likely be developed or redesigned using DB2. Currently, most application systems in DB2 are not heavy volume systems. However, major financial systems developed by Walker Interactive Products Systems are being slated for conversion to DB2 in 1996. These are among the largest of the Corporation's application systems requiring optimum performance to handle the large volume of daily input and inquiries.

Our review of the maintenance processes and parameters in effect in the current DB2 subsystems disclosed the following areas where changes will be needed to ensure continued optimum performance:

Restrictions and Maintenance of Primary (ACF2) and Group IDs

A user's primary authorization ID is their ACF2 logon ID. When a user requests access to DB2, a secondary ID file is searched to associate the user's ACF2 ID to a preassigned secondary or group ID. Assigning DB2 users to group IDs rather than by their ACF2 ID limits the potentially severe consequence known as the “cascade effect”. If an ID's authority is revoked in DB2, all objects created and/or authorizations granted by that ID are disabled. ACF2 IDs are highly susceptible to removal due to transfers or departures.

Our review of the DB2 production subsystem's (DB2P) authorization catalogues disclosed the use of ACF2 IDs for 6 users. Five of the six logon IDs can not be deleted from the system catalogues as it would cause the disabling of 8 data bases and 13 plans in production. It would also cancel 383 authorizations made by these logon IDs to other group IDs in production. The other ID (JH425 found in DB2P's SYSTABAUTH) could be removed with little impact as it was just recently used for the first time.

We also reviewed ACF2 IDs assigned to group IDs and compared them to the ACF2 data base. The comparison revealed 11 IDs contained in the group ID file that no longer exist in the ACF2 data base. In addition, the group ID file contains 105 logon IDs that have been canceled and 5 that

have expired. Of these, 21 logon IDs had never accessed the mainframe computer system. Three of the logon IDs were assigned data base administrator privileges to four data bases.

Periodic Clean-up of the DB2 System Catalogues

The DB2 system's authorization catalogues allow system and data base administrators to control access to objects. Before users are allowed access to DB2 objects, DB2 checks the applicable authorization catalogues to determine if 'the user has been granted the requested authority. The primary catalogues used for security are briefly described in Appendix A.

Inadequate maintenance of the authorization catalogues can result in weakened access controls and ultimately in performance problems due to the size of the catalogues. Accordingly, we reviewed authorization catalogues for three DB2 subsystems (DB2P, FISP, and a development subsystem) to detect identical authorization entries (ie., where one or more identical entries were recorded). The following table presents the results of our review. Most of the redundant entries were found in SYSTABAUTH and SYSPLANAUTH granting permissions to the same ID or plan. Also, the table presents only those occurrences in which the same permission is recorded 3 or more times.

SYSTEM	OCCURRENCES	TOTAL ENTRIES
DB2P	29	90
FISP	158	617
Development Subsystem	152	599

Our review also found authorization records in DB2's security catalogues for obsolete versions of vendor utilities. Future maintenance procedures should include elimination of authorization records as they generally are not needed once the new version of the software has been tested and approved for use.

Restrictions on the Use of Computer Resources in Ad Hoc Queries

DB2 provides the system installation administrator with parameters to set limits on objects that can be utilized during on-line processing. The parameters are established in the Resource Limit Facility. QMF also allows for setting of governors in it's Resource Table that limit the amount of resources that can be utilized during on-line ad hoc queries.

Review of DB2 installation parameters disclosed that the Resource Limit Facility was turned on. However, the parameter, “NO LIMITS” was specified, effectively bypassing any limits on use of resources. Review of the QMF Resource Table found that limits had been established but the

"Scope" field contain a null value effectively shutting off th e governor.

Current DB2 workload requirements can apparently handle mass ive resource requests. However, in future environments, close attention to requests may be required to maintain performance.

Non-Business Data Bases in the Production Subsystem

Our review also disclosed the existence of non-business data base s residing in the production subsystems. They appear to be vendo r supplied data bases set up for training purposes and are accessible to all users. Non-business data bases should not be maintained in th e production environment.

Recommendation:

We recommend that DBU periodically review the use of ACF2 logon IDs in the DB2 catalogues. With the exception of the five IDs ment ioned above, all other uses of the ACF2 logon ID should be promptly corrected.

As future workload and response times increase, DBU should firs t evaluate the reported conditions to determine their feasibility i n improving DB2 performance befo re implementing more costly alternatives.

Auditee Response:

DBU, in conjunction with the S ecurity Administration Section (SAS), has been periodically reviewing all logon IDs in the DB2 catalogues t o determine if any should be deleted. This practice became effective on 12/31/95 and continues on a <u>monthly</u> basis.

DB2 performance reports will be monitored on a weekly basis and th e system will be tuned on a quarterly basis or as required for maximu m efficiency. The initial tuning will be completed by 3/31/96 (Thi s actio n was completed per DIRM's April 3, 1996, response to the draf t report).

DBU will remove all vendor-supplied non-business databases from th e production environment, and wi ll archive these databases for use during maintenance upgrade testing, by 4/30/96.

7. DB2 Subsystem Support Procedures Are Not Documented

DBU has not documented the DB2 subsystem back-up, performance, an d maintenance procedures. Our analysis of the procedures used by DB U found that the procedures were comprehensive and adequately support the DB2 environment. However, the procedures need to be documen ted so that: (1) management maintains accountability controls to ensure thes e

procedures are consistently performed, (2) management can review and determine if the controls are complete or need to be modified to support the changing DB2 environment, and (3) standards supporting DB2 resources will be maintained even though staff changes may occur due to DIRM reorganization or FDIC downsizing.

Presently, DBU has assigned two system administrators the responsibility for subsystem maintenance, performance, and back-up. The administrators, using BMC software, have designed numerous automated thresholds that monitor and correct performance problems. Additionally, the administrators follow thru on various subsystem support issues requiring manual intervention. Examples include:

- periodic review to determine adequacy of all DB2 table backups;
- daily review of critical maintenance indicators;
- standard error correction procedures when performance or maintenance problems arise.

These comprehensive automated and maintenance procedures have been developed thru extensive classroom and on-the-job training, however they have not been documented and thus are not formally established as DBU standards. Without documentation, management loses the accountability controls whereby they can assure these standard procedures are consistently performed. More importantly, the present FDIC downsizing process may reorganize responsibilities such that present DB2 administrators are not assigned DB2 responsibilities thereby losing these undocumented DB2 support techniques. Furthermore, DB2 staff may be reduced and inadvertently result in eliminating many of these present support procedures. Additionally, considering that all RTC data is supported by DB2 and that all FDIC financial data will be supported by DB2, FDIC management should ensure DB2 subsystem support procedures are documented and consistently applied.

Recommendation:

The DB2 system administrators should document present automated and manual performance, maintenance, and backup procedures. DBU management should review, approve, and assure their consistent application.

Auditee Response:

DIRM concurs with this finding. DBU has initiated a project to document the procedures we have in place and ensure that future procedures are documented. Further, we will add a review of these procedures to our internal controls. This project will be completed by 5/01/96.

DB2 SYSTEM AUTHORIZATION CATALOGUES

CATALOGUE NAME	DESCRIPTION
SYSUSERAUTH	Records DB2 system privileges held by users
SYSDBAUTH	Records privileges held by users over data bases
SYSTABAUTH	Records privileges held by users on tables and views
SYSPLANAUTH	Records privileges held by users over plans
SYSCOLAUTH	Records the update privileges held by users on individual columns of a table or view
SYSRESAUTH	Records privileges held by users over buffer pools, storage groups, tablespaces, and collections
SYSPACKAUTH	Records privileges held by users over application packages